Yui Kee Computing Ltd.

Newsletter

June 2012

Contents

Broken Security Models

<web-link for this article>

Allan Dyer

Flame, along with Stuxnet and DuQu are continuing to generate a lot of discussion about the value of different security models, particularly the reactive model that is the major part of most anti-virus products. Naturally, antivirus expert Mikko Hyppönen's admission that the antivirus industry had failed on Stuxnet, Duqu and Flame drew a lot of attention. Mikko has qualified the admission with a longer explanation in wired, saying. "consumer-grade antivirus products can't protect against targeted malware created by well-resourced nation-states with bulging budgets. They can protect you against run-of-the-mill malware".

Security expert Bruce Schneier has responded to Mikko's article, saying, "Probably the people who wrote Flame had a larger budget than a large-scale criminal organization, but their evasive techniques weren't magically better".

I think these are both valid points of view, and the full articles are well worth reading for deeper understanding of the issues. What I would like to add is a warning against less thoughtful commentators who conclude, "therefore we should get rid of reactive antivirus". Mikko's honesty about his industry failing in these cases has distracted attention from failure of other security models in the same cases:

- Whitelisting / Code signing / walled gardens: malware modules were signed with forged or stolen certificates.
- Keeping your software patched: Flame pretended it was a genuine MS update.
- Keeping your software unchanged: Then you fall to the zero-day vulnerabilities present when you started.
- Not networking: Stuxnet spread on USB memory. There's no such thing as an isolated system, there never was.

I am not advocating disregarding these, they are all of some use in our security policy. We should try to get our software from trusted sources, not make unnecessary changes to

production systems, limit access to sensitive systems, and search for known malware. In short, practise defence in depth and always remember that each layer is flawed.

What the antivirus industry must do now is look for ways to identify the slow, stealthy attacks like Stuxnet, DuQu and Flame in among the mountains of samples they constantly receive. It is going to be a difficult job.

More Information

Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet
The Failure of Anti-Virus Companies to Catch Military Malware
Schneier spanks AV industry over Flame failures
Microsoft 'hardens' Windows Update from Flame penetration
Flame, Failure of the Antivirus Industry and Cyber Cold War

June Hong Kong Honeypot Report

<web-link for this article>

This is the sixth monthly report from West Coast Labs's honeypot in Hong Kong, providing some indication of the type and level of malware threat in Hong Kong, but it is only based on a single honeypot, so the conclusions should be treated with caution. This month, Taiwan is the top attack source, but the United States and Japan tie for second. The number of attacks has fallen slightly.

Average Time To Infect: 11 hours 6 minutes

The average time to infect is an indication of how long it would be before a vulnerable computer connected to the internet in Hong Kong became infected.

Summary

Total number of attacks : 67

23 are brand new to this honeypot.

Source of Attacks

The following breaks down where these attacks have come from by use of IP geolocation.

20	Taiwan
13	United States
13	Japan
4	Singapore
3	Canada
1	South Korea
1	France
1	Sri Lanka
1	Hong Kong
1	Malaysia
1	Indonesia
1	India
1	Australia
1	Cambodia

1	Vietnam
1	Hungary
1	Ukraine
1	Israel
1	Switzerland

Malware

Checksum (md5)	This month	Previous count	Detection*
15965bb88165d1eb06851d8f076130ba	4	10	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
75f2a6be36973cc9f3e1cc2a821bb05b	1	1	Y (w32/autorun.aj.gen!eldorado , Backdoor.Win32.Floder.gmq Trojan.Win32.Jorik.IRCbot.gwe , ,)
6527ce860cd40ceda4e2a81782d46c2c	1	0 ***NEW	Y (W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)
94109e9b3f2b045350db9a5cb592b178	2	6	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
c89ff74dfe8aff4bc176106a51f05110	1	0 ***NEW	Y (w32/virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
bbb5034e33568e100dd3dadabb5a57e9	4	8	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
f9dc3945bdd7406bd8db06a47963ec14	4	13	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
3f0fee7c18c9aa7763f44045c52d4be3	1	0 ***NEW	Y (w32/virut.ag , Virus.Win32.Virut.at Net-Worm.Win32.Allaple.e , ,)
cb576cca04946b3d0829703d108ae270	5	9	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
f14a2e20de2c62ef68e2e68ead377398	2	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
3875b6257d4d21d51ec13247ee4c1cdb	3	23	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
e2a1e197bed7e57ec3094d87636797da	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd Backdoor.Win32.Rbot.adqd , ,)
c5ff7232868333107fa3efe895f12361	2	2	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
6add73efbe973a02cc1036568923f377	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd backdoor.win32.rbot.adqd , ,)
d9d4c7a42f91d94665b65598895ffe32	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
6e2fa9031a05b9649da062c550d14a3d	1	2	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
865915650a85e7c27cdd11850a13f86e	3	7	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
54f83c5a2d52482a8c60df30487a6e50	1	0 ***NEW	Y (, Trojan.Win32.Jorik.IRCbot.msf , ,)
b43ad71209c5100b9ed71edb10041514	4	4	N (, , ,) an older file with limited detection
b82698a30e07fc71349f06750cae2664	1	4	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
809fe9b32845edf5c09b871e0e68f227	2	2	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe

			Backdoor.Win32.Rbot.bqj , ,)
2016f3f8bae9ff3044c2d53a580a591c	1	0 ***NEW	Y (w32/virut.7116 , Virus.Win32.Virut.av , ,)
de7c46aca53ed3eb84295405dfc8d72b	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
82c7266ff4dd5ccd348a4056feb5eb05	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.a , ,)
c7f024ddc8200fcb7fabd372c2804a4b	1	0 ***NEW	Y (w32/emailworm.amv , Net-Worm.Win32.Allaple.d , ,)
7d5b46b8c8a4757c2af5348ff9fbffbe	1	0 ***NEW	Y (W32/Virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
b8faf7ea2cd91a318e070f224b439312	1	0 ***NEW	Y (w32/virut.7116 , Virus.Win32.Virut.av , ,)
95262bd40b2be4a9c2ef328e14286d00	1	0 ***NEW	N (, , ,)
f11d86b86efb1d523a07ec8bcb94a61e	1	2	N (, , ,) a new file with no detection
be26cb9839249fb9201c4df0a3d74669	1	0 ***NEW	Y (w32/virut.7116 w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd , ,)
74473505ef968e2f8cd764d9af12adb2	1	1	Y (W32/Allaple.H , Net-Worm.Win32.Allaple.e , ,)
ebdc5a80a546740740f86017bb4ef7b8	1	0 ***NEW	Y (, Backdoor.Win32.Azbreg.aag , ,)
860100849e6962873f097d8d92e1ca33	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
6e9924223fb797722cf654f80640ec43	2	0 ***NEW	Y (, HEUR:Trojan.Win32.Generic , ,)
a0f7bc4600b926cc466c3f1328482088	1	1	Y (w32/virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
3c3011089708c7a49346f648f1e79384	1	0 ***NEW	Y (w32/trojan2.kexn , Trojan-Spy.Win32.Agent.bmxb , ,)
cb2ef50637b9fa9c51d1d6d09a300899	1	0 ***NEW	Y (w32/genbl.cb2ef506!olympus , HEUR:Trojan.Win32.Generic , ,)
3dd2c2b97fc8824ebc7c770752899bed	3	0 ***NEW	Y (, Trojan.Win32.Jorik.Poebot.eq , ,)
c0276991baff7a50b6f774d7055c440b	1	0 ***NEW	Y (W32/Allaple.H , Net-Worm.Win32.Allaple.e Virus.Win32.Virut.n , ,)
2c7ebd64fccf9e0414ae24190839575c	1	1	N (, , ,) a recent file with no detection

One of these files has been in the Wildlist.

Note:

The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

More Information

January Hong Kong Honeypot Report

West Coast Labs

YUI KEE 銳基電腦顧問有限公司 Anti-Virus, Network Security & Education

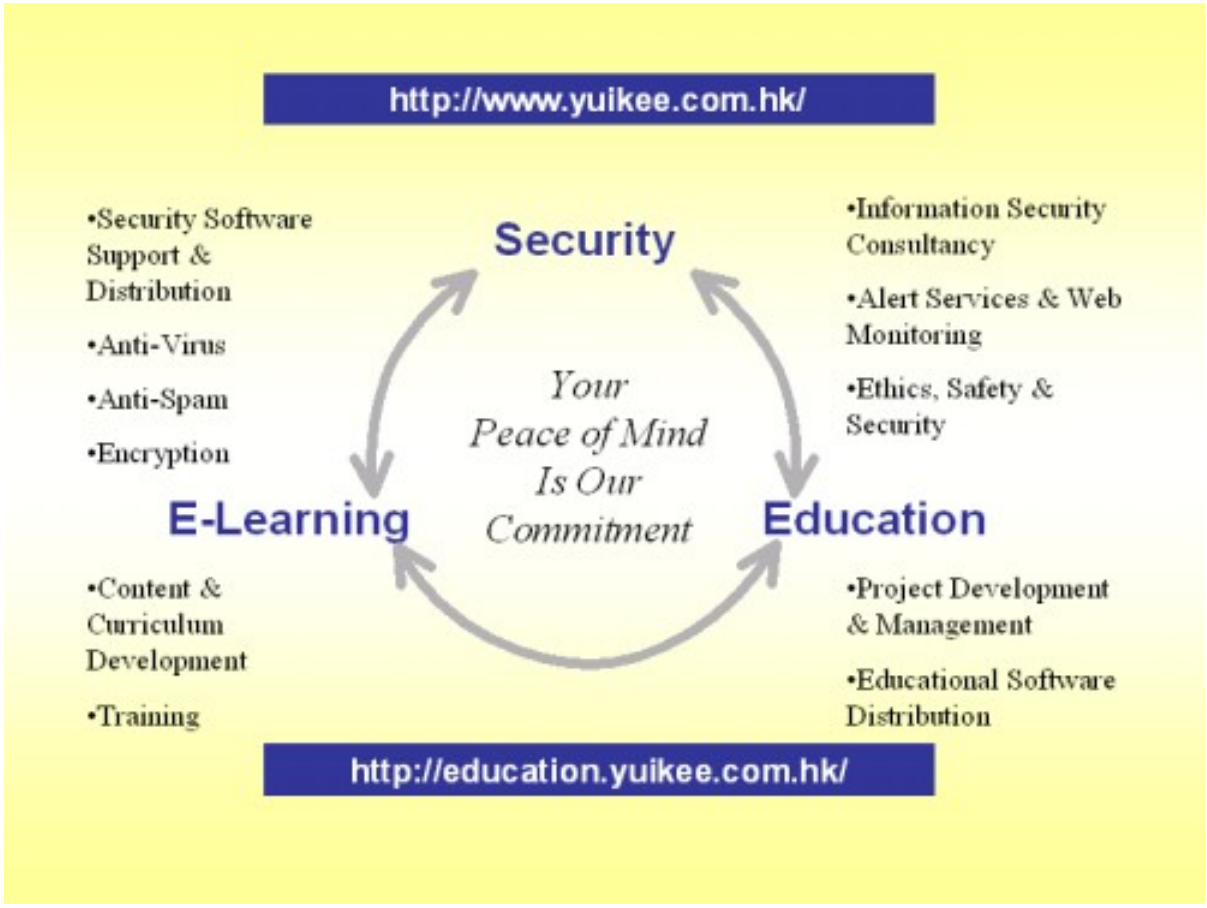
Suite C & D, 8/F, Yally Industrial Building

6 Yip Fat Street, Wong Chuk Hang, Hong Kong

Tel: 2870 8550 Fax: 2870 8563

E-mail: info@yuikee.com.hk

http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/